SHIMURA CURVES OVER FINITE FIELDS AND THEIR RATIONAL POINTS(Algebraic Number Theory and Related Topics)

AUTHOR(S):

IHARA, YASUTAKA

数理解析研究所講究録
1026 巻 1998 年 127-135

SHIMURA CURVES OVER FINITE FIELDS AND THEIR RATIONAL POINTS

YASUTAKA IHARA

0. INTRODUCTION

This is a brief survey of a series of our old works on the title subject. We assume no prerequisites on Shimura varieties to understand what the main results are. We are going to remind you that just as each torsion-free discrete subgroup of $PSL_2(\mathbb{R})$ with compact quotient determines a compact Riemann surface of genus ≥ 2, each torsion-free discrete subgroup Γ of $PSL_2(\mathbb{R}) \times PSL_2(F_\mathfrak{p})$($F_\mathfrak{p}$: a $\mathfrak{p}$-adic field) with compact quotient, whose projection to each component is dense, determines a proper smooth irreducible curve $\mathbb{X}_\Gamma$ of genus $g \geq 2$ over the finite field $\mathbb{F}_q$, where $q = N(\mathfrak{p})^2$, *together with* a special set S_Γ of $\mathbb{F}_q$-rational points of $\mathbb{X}_\Gamma$ with cardinality $(\sqrt{q}-1)(g-1)$, such that $\Gamma \rightsquigarrow (\mathbb{X}_\Gamma, S_\Gamma)$ is functorial in the obvious sense. Subgroups of Γ with finite indices and finite unramified irreducible coverings of $\mathbb{X}_\Gamma$ over $\mathbb{F}_q$, in which all points of S_Γ decompose completely, correspond bijectively with each other. Moreover the Frobenius element of each closed point of $\mathbb{X}_\Gamma - S_\Gamma$ in these coverings can be described by "the corresponding positive primitive $\mathbb{R}$-elliptic Γ-conjugacy class". It is unknown which $(\mathbb{X}, S)$ corresponds with some Γ, but when $(\mathbb{X}, S) = (\mathbb{X}_\Gamma, S_\Gamma)$, the (finitely presented) discrete group Γ is just so large that a certain group-theoretically characterizable conjugacy classes ("positive primitive ... ") of Γ correspond *bijectively* with the closed points of $\mathbb{X} - S$, via Frobenius correspondences in this tower of coverings. On the one hand, this gives an equality between the zeta function of $\mathbb{X}_\Gamma - S_\Gamma$ and a Selberg type zeta function of Γ. From the point of view of the main subject of this conference, this theory can be regarded as giving the first known series of examples of curves over finite fields with many rational points ($q = p^{2f}$ (even power) fixed, $g \to \infty$). Our description of Frobenius elements of closed points of $\mathbb{X}_\Gamma - S_\Gamma$ in terms of Γ can be used to check whether $\mathbb{X}_\Gamma$ has more $\mathbb{F}_q$-rational points than S_Γ. It is a series of old works (conjectured during 1960's, proved during the 70's using works of Shimura, Morita and others), but because of close connections with the main subject of this conference, and because of rather scattered references, we shall take this opportunity and give a brief survey (somewhat more general than as described above), together with a guidance to references.

1. THE DISCRETE SUBGROUPS

The basic datum defining each commensurability class of discrete subgroups Γ is a pair of a quaternion algebra B over a totally real number field F and a non-archimedean place $\mathfrak{p}$ of F satisfying certain conditions. Let

F: a totally real number field, $d = [F : \mathbb{Q}]$,

$\infty_i (1 \leq i \leq d)$: the embeddings $F \hookrightarrow \mathbb{R}$ into the reals,

$\mathfrak{p}$: a non-archimedean place of F,

$F_\mathfrak{p}$: the $\mathfrak{p}$-adic completion of F.

Let B be a quaternion algebra over F which is *unramified* at ∞_1 and $\mathfrak{p}$, and *ramified* at $\infty_2, \cdots, \infty_d$. In other words, B is an algebra over F such that

$$(1) \qquad B \otimes_{F,\infty_1} \mathbb{R} \tilde{\to} M_2(\mathbb{R}), \quad B \otimes_{F,\mathfrak{p}} F_\mathfrak{p} \tilde{\to} M_2(F_\mathfrak{p})$$

but that

$$(1)' \qquad B \otimes_{F,\infty_i} \mathbb{R} \not\to M_2(\mathbb{R}) \quad (2 \le i \le d),$$

where $M_2(\ )$ denotes the matrix algebra of degree 2. (A word about the existence and a parametrization of such B. For any given finite set $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_r\}$ $(r \ge 0)$ of distinct non-archimedean places of F such that $\mathfrak{q}_j \ne \mathfrak{p}$ $(1 \le j \le r)$ and $d-1+r \equiv 0 \pmod 2$, there exists by the Hasse principle a unique F-isomorphism class of B ramified *exactly* at the places ∞_i $(2 \le i \le d)$ and $\mathfrak{q}_j$ $(1 \le j \le r)$.) Fix two $\mathbb{R}$- (resp. $F_\mathfrak{p}$-) isomorphisms in (1), and call them $i_\mathbb{R}$ (resp. $i_\mathfrak{p}$). Consider a locally compact group

$$(2) \qquad G = G_\mathbb{R} \times G_\mathfrak{p},$$

where

$$(3)_\mathbb{R} \qquad G_\mathbb{R} = PL_2^+(\mathbb{R}) = SL_2(\mathbb{R})/\{\pm 1\},$$

$$(3)_\mathfrak{p} \qquad G_\mathfrak{p} = PL_2^+(F_\mathfrak{p}) = \{g \in GL_2(F_\mathfrak{p}); ord_\mathfrak{p}(\det g) \equiv 0 (mod\ 2)\}/F_\mathfrak{p}^\times$$

($ord_\mathfrak{p}$: the normalized additive discrete valuation of $F_\mathfrak{p}$). Note that $G_\mathfrak{p}$ contains $PSL_2(F_\mathfrak{p}) = SL_2(F_\mathfrak{p})/\{\pm 1\}$ as an open normal subgroup with index a power of 2 (equals to 2 if $\mathfrak{p} \nmid 2$). Define a commensurability class $\mathcal{L}_{B,\mathfrak{p}}$ of discrete subgroups of G as follows. Let $\mathfrak{O}_F^{(\mathfrak{p})} = \cup_{n \ge 0} \mathfrak{p}^{-n} \mathfrak{O}_F$ ($\mathfrak{O}_F$: the ring of integers of F), and let $\mathfrak{O}$ be any $\mathfrak{O}_F^{(\mathfrak{p})}$-*order* in B, *i.e.*, a subring of B containing 1 which is a finite $\mathfrak{O}_F^{(\mathfrak{p})}$-module satisfying $F \cdot \mathfrak{O} = B$. Put

$$(4) \qquad \Gamma(\mathfrak{O}) = \{\gamma \in \mathfrak{O}; N_{B/F}(\gamma) = 1\}/\{\pm 1\} \underset{via\ i_\mathbb{R} \times i_\mathfrak{p}}{\hookrightarrow} G.$$

Here, $N_{B/F}$ is the reduced norm, which corresponds with the matrix determinant via (1). Let $\mathcal{L}_{B,\mathfrak{p}}$ denote the set of all subgroups Γ of G that are *commensurable with* $\Gamma(\mathfrak{O})$ (i.e., $\Gamma \cap \Gamma(\mathfrak{O})$ has finite indices both in Γ and in $\Gamma(\mathfrak{O})$). Then $\mathcal{L}_{B,\mathfrak{p}}$ is independent of the choice of $\mathfrak{O}$. It depends on $i_\mathbb{R}, i_\mathfrak{p}$, but the effect of changing these isomorphisms is merely that $\mathcal{L}_{B,\mathfrak{p}}$ is replaced by its conjugate by an element of $PL_2(\mathbb{R}) \times PL_2(F_\mathfrak{p})$. Each $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ is a discrete subgroup of G whose quotient G/Γ has a finite invariant volume. The projections $\Gamma \to G_\mathbb{R}, \Gamma \to G_\mathfrak{p}$ are always injective, and the image is dense in $G_\mathbb{R}$ (resp. the closure of the image in $G_\mathfrak{p}$ contains $PSL_2(F_\mathfrak{p})$). Moreover,

(i) *the initial data* $F, \infty_1, B, \mathfrak{p}$ *can be recovered from* $\mathcal{L}_{B,\mathfrak{p}}$;

(ii) *all irreducible lattices in* G *are obtained this way* (a special case of Margulis [Ma]).

Here, by an *irreducible* lattice in G, we mean a discrete subgroup $\Gamma \subset G$ such that G/Γ has finite invariant volume, which is not commensurable with a product of discrete subgroups of $G_\mathbb{R}$ and of $G_\mathfrak{p}$.

When $F = \mathbb{Q}$ and $B = M_2(\mathbb{Q})$, $\mathcal{L}_{B,p}$ is the commensurability class of discrete subgroups of $PL_2^+(\mathbb{R}) \times PL_2^+(\mathbb{Q}_p)$ represented by $PSL_2(\mathbb{Z}[\frac{1}{p}])$. This case is referred to as the *elliptic modular* case. In this case, G/Γ is non-compact. In other cases, B is a division algebra, and G/Γ is compact for any $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ (referred to as the *division* case).

In each case, each $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ contains a subgroup of finite index which is torsion-free. We shall denote by $\mathcal{L}^0_{B,\mathfrak{p}}$ the subset of $\mathcal{L}_{B,\mathfrak{p}}$ formed of all such $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ that are *torsion-free*. Each group $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ is residually finite, i.e., the intersection of all subgroups of Γ with finite indices reduces to $\{1\}$, or equivalently, the canonical homomorphism $\Gamma \to \hat{\Gamma}$ to the profinite completion is injective.

Let F^{ab} denote the maximal abelian extension of F (in $\mathbb{C}$, w.r.t. ∞_1). We shall pick and *fix* an extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$ in F^{ab}.

2. The main results

Main Theorem. *Let B/F, $\mathfrak{p}$, $\tilde{\mathfrak{p}}$, $i_{\mathbb{R}}$, $i_{\mathfrak{p}}$ be as above, and put $q = N(\mathfrak{p})^2$. Then:*

(i) *To each $\Gamma \in \mathcal{L}^0_{B,\mathfrak{p}}$ is canonically associated a triple $\mathcal{X}_\Gamma = (\mathbb{X}_\Gamma; S_\Gamma, T_\Gamma)$, where*

$\mathbb{X}_\Gamma$: *a proper smooth irreducible curve over $\mathbb{F}_q$,*

$S_\Gamma \subset \mathbb{X}_\Gamma(\mathbb{F}_q)$: *a non-empty set of $\mathbb{F}_q$-rational points of $\mathbb{X}_\Gamma$ (called "special points"),*

$T_\Gamma \subset \mathbb{X}_\Gamma(\bar{\mathbb{F}}_q) - S_\Gamma$: *a finite set of points (called "cusps"), stable under conjugations over $\mathbb{F}_q$; $T_\Gamma = \varnothing \Leftrightarrow$ the division case.*

It is such that there exists a rational differential ω_Γ on $\mathbb{X}_\Gamma$ of order $\sqrt{q}-1$, holomorphic outside T_Γ (i.e., an element of $H^0(\mathbb{X}_\Gamma - T_\Gamma, (\Omega^1_{\mathbb{X}_\Gamma})^{\otimes(\sqrt{q}-1)})$), whose divisor is

$$(\omega_\Gamma) = 2S_\Gamma - (\sqrt{q}-1)\,T_\Gamma; \tag{5}$$

in particular, the cardinality of S_Γ is given by

$$\#(S_\Gamma) = (\sqrt{q}-1)(g_\Gamma - 1 + \frac{1}{2}\#(T_\Gamma)), \tag{6}$$

g_Γ being the genus of $\mathbb{X}_\Gamma$.

The association $\Gamma \mapsto \mathcal{X}_\Gamma$ is functorial in the following sense. For any $\Gamma, \Gamma' \in \mathcal{L}^0_{B,\mathfrak{p}}$, there is a canonical bijection

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma', \Gamma) & \approx & \mathrm{Hom}(\mathcal{X}_{\Gamma'}, \mathcal{X}_\Gamma) \\ \| & & \| \\ \{\Gamma g\ (g \in G);\ g\Gamma' g^{-1} \subset \Gamma\} & & \{f : \mathbb{X}_{\Gamma'} \to \mathbb{X}_\Gamma,\ \text{a finite } \mathbb{F}_q\text{-morphism s.t. } f^{-1}(S_\Gamma) = S_{\Gamma'},\ f^{-1}(T_\Gamma) = T_{\Gamma'},\ f: \text{tamely ramified, and unramified outside } T_\Gamma\}. \end{array} \tag{7}$$

(ii) *Conversely, if $\Gamma \in \mathcal{L}^0_{B,\mathfrak{p}}$ and if $f : \mathbb{X}' \to \mathbb{X}_\Gamma$ is a finite irreducible tamely ramified covering over $\mathbb{F}_q$, unramified outside T_Γ, such that*

$$f^{-1}(S_\Gamma) \subset \mathbb{X}'(\mathbb{F}_q), \tag{8}$$

then there exists $\Gamma' \subset \Gamma$ with finite index such that $\mathbb{X}' = \mathbb{X}_{\Gamma'}$ and that f corresponds with $\Gamma \cdot 1 \in \mathrm{Hom}(\Gamma', \Gamma)$. In particular, as for the profinite completion $\hat{\Gamma}$ of Γ,

$$\hat{\Gamma} \xrightarrow{\sim} \pi_1^{tame}(\mathbb{X}_\Gamma - T_\Gamma)/(\textit{Frobenius conjugacy classes above } S_\Gamma), \tag{9}$$

where $\pi_1^{tame}(\ \ )$ denotes the tame fundamental group.

(iii) *There is a canonical bijection*

(10)

$$\begin{array}{ccc} \{\mathbb{X}_\Gamma(\bar{\mathbb{F}}_q) - S_\Gamma - T_\Gamma\}/\mathbb{F}_q\text{-conjugacy} & \approx & \left\{\begin{array}{c}\text{"Positive primitive } \mathbb{R}\text{-elliptic"} \\ \Gamma\text{-conjugacy classes}\end{array}\right\} \\ P & \longleftrightarrow & c_P \end{array}$$

such that the $\hat{\Gamma}$*-conjugacy class determined by* c_P *is the Frobenius element of* P *in* $\hat{\Gamma}$. *Here, a* Γ*-conjugacy class, represented by* $\gamma \in \Gamma$, *is called* $\mathbb{R}$-elliptic *if the projection* $\gamma_{\mathbb{R}}$ *of* γ *on* $G_{\mathbb{R}}$ *has imaginary eigenvalues* $\pm\{\lambda, \lambda^{-1}\}$, primitive *if* γ *generates its centralizer in* Γ, *and* positive *if* $\mathrm{ord}_{\mathfrak{p}}(\lambda) > 0$, *where* λ *is so chosen that the corresponding eigen (column) vector* ${}^t(\omega_1, \omega_2)$ *has the property* $\mathrm{Im}(\omega_1/\omega_2) > 0$. *This bijection preserves the degree,*

$$\deg P = \deg c_P, \tag{11}$$

where $\deg P$ *is the degree of* P *over* $\mathbb{F}_q$, *and* $\deg c_P = \mathrm{ord}_{\mathfrak{p}}(\lambda)$.

3. Various remarks

(A) The above theorem can be generalized to the case where $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ has torsion, but the description becomes more complicated. The basic fact is that when $\Gamma \in \mathcal{L}_{B,\mathfrak{p}}$ and Γ' is a torsion-free normal subgroup of Γ with finite index, Γ/Γ' acts on $\mathcal{X}_{\Gamma'}$ (via (7) for $\mathrm{Hom}(\Gamma', \Gamma')$) and $\mathcal{X}_\Gamma$ is its quotient.

(B) The above isomorphism (9) (in Theorem (ii)) gives some informations on $\pi_1^{\mathrm{tame}}(\mathbb{X}_\Gamma - T_\Gamma)$. Note that this is *not* restricted to the prime-to-p part.

(C) By Theorem (iii), we can compute $\#\mathbb{X}_\Gamma(\mathbb{F}_{q^m})$ $(m \geq 1)$ knowing Γ but without knowing explicit equations defining the curve $\mathbb{X}_\Gamma$.

(D) *The congruence subgroup property for* Γ. Whether every subgroup of Γ with finite index contains some congruence subgroup (congruences in the orders of the corresponding quaternion algebra B) is generally unknown. This is known to be valid when $B = M_2(\mathbb{Q})$ (Mennicke $(p = 2)$, Serre (general) [Se_1]), but unknown in the division quaternion cases. When $\Gamma = PSL_2(\mathbb{Z}[\frac{1}{p}])$, by this property, $\hat{\Gamma} \cong (\prod_{l \neq p} SL_2(\mathbb{Z}_l))/\{\pm 1\}$.

(E) *Advantages of relating to* Γ. Theorem (iii) is one of them. That Theorem (ii) can be proved without using the congruence subgroup property for Γ, is also an advantage of using Γ (instead of its adelic version).

(F) *Many* $\mathbb{F}_q$*-rational points.* The curve $\mathbb{X}_\Gamma$ has at least

$$(\sqrt{q} - 1)(g_\Gamma - 1)$$

number of $\mathbb{F}_q$-rational points. This gave rise to the inequality

$$A(q) \geq \sqrt{q} - 1 \qquad \text{(cf. [I}_{11}\text{])}$$

for $q = p^{2f}$.

(G) We know more about the structure of the set S_Γ (esp. its relation with the canonical divisor). Can we not make use of this for further applications to coding theory? For example, the above theorem gives immediately:

$$\mathrm{Jac}(\mathbb{X}_\Gamma)(\mathbb{F}_q)/\langle s - s';\ s, s' \in S_\Gamma\rangle \cong {}_{canon}\Gamma^{ab}, \tag{12}$$

where $\mathrm{Jac}(X_\Gamma)$ is the Jacobian variety, and Γ^{ab} is the abelianization of Γ (which is always finite and is computable).

4. How to construct $\mathcal{X}_\Gamma$ from Γ

As is well-known, $G_\mathfrak{p} = PL_2^+(F_\mathfrak{p})$ is a free product of two maximal compact subgroups

$$U_\mathfrak{p} = PL_2(\mathcal{O}_\mathfrak{p}) = GL_2(\mathcal{O}_\mathfrak{p})/\mathcal{O}_\mathfrak{p}^\times \quad \text{and} \quad U'_\mathfrak{p} = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}^{-1} U_\mathfrak{p} \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} \tag{13}$$

with amalgamated subgroup $U_\mathfrak{p}^0 = U_\mathfrak{p} \cap U'_\mathfrak{p}$, where $\mathcal{O}_\mathfrak{p}$ is the ring of integers of $F_\mathfrak{p}$ and π is a prime element of $F_\mathfrak{p}$. More intrinsically, the $G_\mathfrak{p}$-conjugacy class of the pair $\{U_\mathfrak{p}, U'_\mathfrak{p}\}$ can be understood as the pair of stabilizers of adjascent vertices of the (regular bipartite) tree associated with $G_\mathfrak{p}$. Let $\Delta, \Delta', \Delta^0 = \Delta \cap \Delta'$ be the pull-backs of $U_\mathfrak{p}, U'_\mathfrak{p}, U_\mathfrak{p}^0$, respectively, via the projection $\Gamma \to G_\mathfrak{p}$, and for any subgroup $H \subset \Gamma$, let $H_\mathbb{R}$ denote the image of H under the (injective) projection $\Gamma \to G_\mathbb{R}$. Then $\Delta_\mathbb{R}, \Delta'_\mathbb{R}, \Delta^0_\mathbb{R}$ are discrete subgroups of $G_\mathbb{R}$ with finite-volume quotients, and $\Gamma_\mathbb{R}$ is a free product of $\Delta_\mathbb{R}$ and $\Delta'_\mathbb{R}$ with amalgamated subgroup $\Delta^0_\mathbb{R}$. The group $G_\mathbb{R}$ acts on the Poincaré upper half plane $\mathcal{H}$ in the usual manner, and the quotients $\Delta_\mathbb{R}\backslash\mathcal{H}, \Delta'_\mathbb{R}\backslash\mathcal{H}, \Delta^0_\mathbb{R}\backslash\mathcal{H}$ are compact (resp. can be compactified by addition of finitely many cusps) according to whether $B \not\simeq M_2(\mathbb{Q})$ (resp. $B \simeq M_2(\mathbb{Q})$). Call $\mathcal{R}, \mathcal{R}', \mathcal{R}^0$ the compact Riemann surfaces thus obtained from $\Delta_\mathbb{R}, \Delta'_\mathbb{R}, \Delta^0_\mathbb{R}$, respectively, considered also as complex algebraic curves, and call $\varphi : \mathcal{R}^0 \to \mathcal{R}$, $\varphi' : \mathcal{R}^0 \to \mathcal{R}'$ the projections which are of degree $N(\mathfrak{p}) + 1 (= (U_\mathfrak{p} : U_\mathfrak{p}^0) = (U'_\mathfrak{p} : U_\mathfrak{p}^0))$. When $\Gamma = PSL_2(\mathbb{Z}[\frac{1}{p}])$,

$$\Delta_\mathbb{R} = PSL_2(\mathbb{Z}), \quad \Delta'_\mathbb{R} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Delta_\mathbb{R} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \tag{14}$$

$$\Delta^0_\mathbb{R} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_\mathbb{R};\ c \equiv 0 \pmod{p} \right\},$$

and hence $\mathcal{R}$ is the (compactified) complex j-line, $\mathcal{R}'$ can be identified with $\mathcal{R}$ (via the automorphism $\tau \to p\tau$ of $\mathcal{H}$), and $\mathcal{R}^0$ is the normalization of the graph on $\mathcal{R} \times \mathcal{R}$ of the modular equation of degree p. In general, thanks to Shimura [Sh_1][Sh_2] (esp. [Sh_2]), we know that there is a standard model of each of $\mathcal{R}, \mathcal{R}', \mathcal{R}^0, \varphi, \varphi'$ over the maximal abelian extension F^{ab} of F, and moreover that each curve (say $\mathcal{R}$) has various models over subextensions of F^{ab}/F depending on the choice of adelic open compact subgroups U_A of $B_A^\times$ (the adele group of $B^\times$) with which "$pr_{\infty_1}(U_A \cap (B^\times)^+) = \Delta_\mathbb{R}$". Here, we choose what we called the "$\mathfrak{p}$-canonical model". Let $F^{(\mathfrak{p})}$ denote the decomposition field of $\mathfrak{p}$ in F^{ab}/F, and $F^{(\mathfrak{p}^2)}/F^{(\mathfrak{p})}$ the unique quadratic subextension in $F^{ab}/F^{(\mathfrak{p})}$ in which $\tilde{\mathfrak{p}}$ is unramified. Then there is a canonical model of the system

$$\mathcal{R} \xleftarrow{\varphi} \mathcal{R}^0 \xrightarrow{\varphi'} \mathcal{R}' \tag{15}$$

over $F^{(\mathfrak{p}^2)}$ ([I_8], I§6). The key word for the definition is "divide by the scalars $F_\mathfrak{p}^{\times''}$". Its conjugate over $F^{(\mathfrak{p})}$ is the transpose of (15). So far, the objects constructed depend on Γ and $\mathfrak{p}$ but not on $\tilde{\mathfrak{p}}$. But the next object, *i.e.*, the system of curves obtained by reduction mod $\tilde{\mathfrak{p}}$ of (15), will depend on the choice of an extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$. By Shimura [Sh_2], Morita [Mo] and others (cf. [I_{12}, (§4)], it is known that $\mathcal{R}$

has a good reduction at $\tilde{\mathfrak{p}}$ (call it $\mathbb{X}$), and moreover that the reduction mod $\tilde{\mathfrak{p}}$ of (15) can be described as follows:

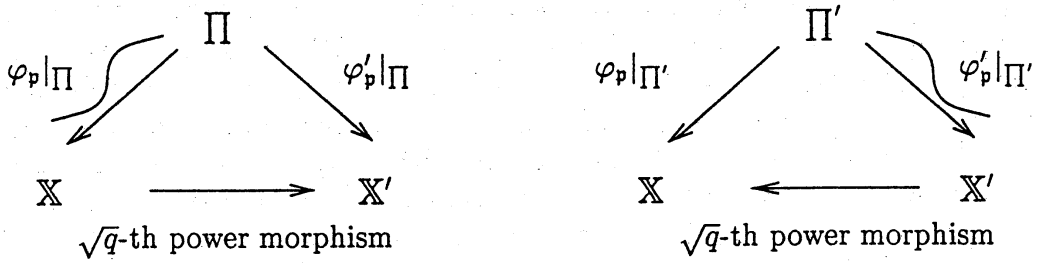
$$(15)_{\tilde{\mathfrak{p}}} \qquad \mathbb{X} \xleftarrow{\varphi_{\mathfrak{p}}} \prod \cup \prod' \xrightarrow{\varphi'_{\mathfrak{p}}} \mathbb{X}'$$

$\mathbb{X}$: a proper smooth irreducible curve over $\mathbb{F}_q$ ($q = N(\mathfrak{p})^2$),

$\mathbb{X}'$: the $\mathbb{F}_{\sqrt{q}}$-conjugate of $\mathbb{X}$,

$\varphi_{\mathfrak{p}}|_{\prod}, \varphi'_{\mathfrak{p}}|_{\prod'}$ are isomorphisms, and $(15)_{\tilde{\mathfrak{p}}}$ induces the following two commutative diagrams

(16)



The intersection $\prod \cap \prod'$ is non-empty, and $\prod, \prod'$ meet transversally at each point of $\prod \cap \prod'$. The projection $S_\Gamma = pr_X(\prod \cap \prod')$ is a non-empty subset of $X(\mathbb{F}_q)$. When $B \cong M_2(\mathbb{Q})$, cusps on $\mathcal{R}$ are algebraic points, and the reduction mod $\tilde{\mathfrak{p}}$ of cusps is injective, and the image is, by definition, T_Γ. A key lemma for the proof of Theorem (i)(ii) is that the strict categorical equivalence holds among

(a) subgroups with finite indices of Γ,
(b) finite etale coverings of the system (15)
(c) finite etale coverings of the system $(15)_{\tilde{\mathfrak{p}}}$ ([I$_8$],II§4).

The equivalence between (a) and (b) follows from the fact that Γ is a free product of Δ and Δ' with amalgamated subgroup Δ^0, while that between (b) and (c) is quite delicate, because we include the case where the degree of the covering is divisible by p. A result of [I-M] is essential.

About the bijection (10). The association $\{\gamma\}_\Gamma \to P$ is defined as follows. The projection $\gamma_{\mathbb{R}}$ of γ on $G_{\mathbb{R}}$ has a unique fixed point z on $\mathcal{H}$ (because of the $\mathbb{R}$-ellipticity of γ). The projection of z on $\mathcal{R} = \Delta_{\mathbb{R}}\backslash\mathcal{H}$ is F^{ab}-rational (Shimura). Let $P \in \mathbb{X}(\overline{\mathbb{F}}_q)$ be its reduction mod $\tilde{\mathfrak{p}}$. Then the $\mathbb{F}_q$-conjugacy class of P depends only on $\{\gamma\}_\Gamma$, and one can prove that (10) is bijective, using our study of the zeta function of Γ, etc.([I$_1$],[I$_8$]).

Remark 1. Since Γ is a free product of two fuchsian groups Δ, Δ' with amalgamation Δ^0, one knows, in principle, a way of presentation of Γ in terms of generators and relations. Suppose for simplicity that $B \not\cong M_2(\mathbb{Q})$ and that Γ is torsion-free. Let $g = g_\Gamma$, the genus of $\mathcal{R}$ (and of $\mathcal{R}'$). Then $g \geq 2$, and Δ (resp. Δ') has standard generators $a_1, \cdots, a_g, b_1, \cdots, b_g$ (resp. $a'_1, \cdots, a'_g, b'_1, \cdots, b'_g$) which are subject to the relations

$$(17) \qquad [a_1, b_1] \cdots [a_g, b_g] = 1, \quad [a'_1, b'_1] \cdots [a'_g, b'_g] = 1,$$

where $[g, g'] = gg'g^{-1}g'^{-1}$. Now the genus of $\mathcal{R}^0$ is $g^0 = 1 + (\sqrt{q}+1)(g-1)$, and Δ^0 is generated by $2g^0$ elements c_j $(1 \leq j \leq 2g_0)$ (subject to a single similar relation).

Now express each c_j in terms of the a_i, b_i's, and also in terms of a_i', b_i''s:

(18) $(c_j =)F_j(a_1, \cdots, a_g; b_1, \cdots, b_g) = G_j(a_1', \cdots, a_g'; b_1', \cdots, b_g') \quad (1 \leq j \leq 2g^0)$.

Then Γ is generated by the a_i, b_i, a_i', b_i' $(1 \leq i \leq 2g)$, and (17) and (18) give a system of defining relations.

Remark 2. *Which* $(\mathbb{X}, S)$ *corresponds with some* Γ ? This question has not been answered. It is of course closely related to the question of liftability of the system $(15)_{\bar{\mathfrak{p}}}$ to (15), which is studied to some extent in [I7][I9][I10] (esp. [I10]).

5. About the differential ω_Γ

(A) The differential ω_Γ is determined up to $\mathbb{F}_q^\times$-multiples, and is *independent* of the choice of $\Gamma \in \mathcal{L}^0_{B,\mathfrak{p}}$. This is because if $\Gamma' \subset \Gamma$ with $(\Gamma, \Gamma') < \infty$, then $S_{\Gamma'}$ (resp. $T_{\Gamma'}$) consists of all points of $\mathbb{X}_{\Gamma'}$ that lift S_Γ (resp. T_Γ).

(B) The existence of ω_Γ is closely related to the liftability of the system $(15)_{\bar{\mathfrak{p}}}$ to a system modulo $\mathfrak{p}^2$ (see [I7]). Moreover, ω_Γ is closely related to the solution of the reduction mod $\mathfrak{p}$ of the Schwarzian differential equation defining the uniformization $\mathcal{H} \to {}_\Delta\backslash\mathcal{H} = \mathcal{R}$ ([I4][I5]). By using these, one can compute $\mathcal{X} = (\mathbb{X}_\Gamma, S_\Gamma, T_\Gamma)$ explicitly in some special cases ([I5]; see §6 below).

(C) There is also a p-adic differential $\tilde{\omega}_\Gamma^{(1)}$ such that

$$\omega_\Gamma = (\tilde{\omega}_\Gamma^{(1)} (\mathrm{mod}\ \mathfrak{p}))^{\otimes(\sqrt{q}-1)}$$

([I6], cf.[K]§2 for a published version). This $\tilde{\omega}_\Gamma^{(1)}$ lives in a certain complete p-adic field whose residue field is an infinite cyclic extension of the function field $\mathbb{F}_q(\mathbb{X})$ of $\mathbb{X}$ whose Galois group is an open subgroup of $\mathbb{Z}_p^\times$. It is Galois semi-invariant, and defines a character

$$\chi_\Gamma : \pi_1(\mathbb{X}_\Gamma - S_\Gamma) \to \mathbb{Z}_p^\times.$$

6. Examples

Example 1 Let $F = \mathbb{Q}$ and $B/\mathbb{Q}$ be the quaternion algebra ramified exactly at 2 and 3. Let $p \neq 2, 3, \mathcal{O}$ be a maximal $\mathbb{Z}[\frac{1}{p}]$-order in B, and put

$$\Gamma = \{\gamma \in \mathcal{O};\ \underset{B/\mathbb{Q}}{N}(\gamma) = 1, \gamma \equiv 1 (\mathrm{mod}\ \sqrt{6}\mathcal{O})\}/\{\pm 1\},$$

where $\sqrt{6}\mathcal{O}$ is the unique two-sided $\mathcal{O}$-ideal with reduced norm 6. This group Γ is torsion-free. In this case, one can show ([I5] §4.3, [I10] §3.1) that $\mathbb{X}_\Gamma$ is the smooth compactification of the affine curve

$$y^2 = 1 + x^6$$

over $\mathbb{F}_{p^2}$, which is of genus 2, and S_Γ is the set of zeros of a hypergeometric polynomial of degree $p - 1$. For example, if $p \equiv 1 (\mathrm{mod}\ 24)$, S_Γ is the set of zeros of

$$F(\frac{1}{24}, \frac{5}{24};\ \frac{1}{2}; t); \qquad t = \frac{(x^6 - 1)^2}{(-4x^6)}.$$

Here, $F(a, b; c; t) = 1 + \frac{a \cdot b}{1 \cdot c} t + \frac{a(a+1)b(b+1)}{1 \cdot 2 \cdot c(c+1)} t^2 + \cdots (\mathrm{mod}\ p)$, which is truncated to be of degree $\frac{p-1}{24}$ (in t). See [I5] for more details and for other similar examples.

Example 2 $F = \mathbb{Q}(\sqrt{2})$, B/F is ramified exactly at ∞_2, (5).
Let $\mathfrak{p} = (\sqrt{2})$, $\mathcal{O}$ be a maximal $\mathfrak{O}_F^{(p)}$-order in B, and put

$$\Gamma = \{\gamma \in \mathcal{O};\ \underset{B/F}{N}(\gamma) = 1\}/\{\pm 1\}.$$

Then $\mathbb{X}_\Gamma/\mathbb{F}_4$ is of genus 2, $\#(S_\Gamma) = 1$. In this case, I have not been able to compute $\mathbb{X}_\Gamma$ and S_Γ explicitly.

Example 3 $\mathbb{X} \subset \mathbb{P}^2$ over $\mathbb{F}_9$ is a smooth plane quartic defined by the homogeneous equation

$$X^3Y - XY^3 + XYZ^2 + Z^4 = 0.$$

The genus is 3. Let S be the 4 points of $\mathbb{X}$ defined by $Z = 0$. Then $\mathbb{X} \leftarrow \Pi \overset{\cup}{S} \Pi' \rightarrow \mathbb{X}$ is liftable to a system over $\mathbb{Z}_p$ (cf. [I_{10}] §3.1). It is very plausible that this corresponds with some Γ. Find B, Γ for this system !

References

[I_1] Ihara, Y., (a) The congruence monodromy problems, J. Math. Soc. Japan, **20** (1968), 107-121.
(b) On congruence monodromy problems, Lect. Note, Univ. Tokyo, **1** (1968), **2** (1969).
(c) Non-abelian classfields over function fields in special cases, Actes du Congrès Internat. Math. Nice 1970, **1**, 381-389.

[I_2] ———, An invariant multiple differential attached to the field of elliptic modular functions of characteristic p, Amer. J. Math., **93** (1971), 139-147.

[I_3] ———, On modular curves over finite fields, Proc. Intern. Colloq. on Discrete Subgroups on Lie Groups, Bombay, Jan. 1973; Tata Inst. Fund. Research, Studies in Math. 7; Oxford Univ. Press, 1975, 161-202.

[I_4] ———, Schwarzian equations, J. Fac. Sci. Univ. Tokyo, Sect. IA, **21** (1974), 97-118.

[I_5] ———, On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations, J. Fac. Sci. Univ. Tokyo, Sect. IA, **21** (1974), 309-332.

[I_6] ———, (a) Non-abelian invariant differentials (mimeographed note, 1971).
(b) Non-abelian invariant differential and Schwarzian equations in the p-adic theory of automorphic functions, Proc. U.S.-Japan Seminar in "Modern Methods in Number Theory", 1971.

[I_7] ———, On the Frobenius correspondences of algebraic curves, "Algebraic number theory", Papers contributed for the International Symposium, Kyoto, 1976, Japan Soc. Prom. Sci., (1977), 67-98.

[I_8] ———, Congruence relations and Shimura curves, I, Proc. Symp. in Pure Math., **33** Part 2, (1977), 291-311, Amer. Math. Soc.; II, J. Fac. Sci. Univ. Tokyo, Sect. IA, **25** (1979), 301-361.

[I_9] ———, Congruence relations and fundamental groups, J. Algebra, **75** (1982), 445-451.

[I_{10}] ———, Lifting curves over finite fields together with the characteristic correspondence II+II', ibid., **75** (1982), 452-483.

[I_{11}] ———, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo, Sect. IA, **28** (1982), 721-724.

[I_{12}] ———, On unramified extensions of function fields over finite fields, Adv. Studies in Pure Math., **2** (1983) "Galois groups and their representations"; 89-97.

[I-M] Ihara, Y. and Miki, H., Criteria related to potential unramifiedness and reduction of unramified coverings of curves, J. Fac. Sci. Univ. Tokyo, Sect. IA, **22** (1975), 237-254.

[K] Koike, M., Congruences between modular forms and functions, and applications to the conjecture of Atkin, J. Fac. Sci. Univ. Tokyo, Sect. IA, **20** (1973), 129-169.

[Ma] Margulis, G. A., Дискретные Группы Движений Многообразий Неположительной Кривизны, Proc. Internat. Congress Math. (Vancouver 1974) **2**, 21-34.

[Mo] Morita, Y., Reduction mod $\mathfrak{P}$ of Shimura curves, Hokkaido Math. J., **10** (1981), 209-238.

[O] Ohta, M., On l-adic representations attached to automorphic forms, Japanese J. Math., **8** (1982), 1-47.

[Se_1] Serre, J-P., Le problème des groupes de congruence pour SL_2, Ann. of Math., **92** (1970), 489-527.

[Se_2] ———, Arbres, amalgames, SL_2, Astérisque 46, Soc. Math. France, 1977.

[Sh_1] Shimura, G., Construction of class fields and zeta functions of algebraic curves, Ann. of Math., **85** (1967), 58-159.

[Sh_2] ———, On canonical models of arithmetic quotients of bounded symmetric domains I, Ann. of Math., **91** (1970), 144-222; II, ibid., **92** (1970), 528-549.

RIMS, Kyoto University,
Kyoto 606-8502, JAPAN
e-mail: ihara@kurims.kyoto-u.ac.jp